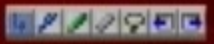
Windows Privacy

Jeffrey Friedberg
Director Windows Privacy
Microsoft Corporation

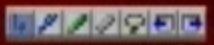


Agenda

- Motivation
- Brief History
- Windows Privacy Initiative
- P3P Discussion
- Objective/Subjective Trust

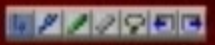
Why Protect Customer Privacy?

- Erosion of trust can hurt sales
  - "Phone Home" became a major deployment blocker
    - CIA, USAF needed disclosure and control
    - University of Florida worried over HIPAA
  - Scary EULA language was catalyst
    - Original DRM clause too broad
    - Automatic downloading counter to managed systems
- Global issue with big stakes
  - EU Privacy Probe
  - FTC Consent Decree
- Doing privacy right can be a market differentiator

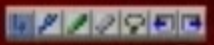


“Phone Home” Effort

- Immediately redrafted DRM EULA text
  - Narrowed scope and added clarifications
- Analyzed components and found 28 that called Microsoft
- Added some missing controls
- Provided disclosure and mitigation strategies in 180 page White Paper
- Turning the corner with customers



Windows Media Player Fiasco



Windows Media Player Fiasco

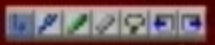
- Forgot to disclose DVD metadata lookup
- Privacy expert: “MS can track what you watch”
  - Packet sniffer uncovered GUID
  - Scenario wasn’t documented

Windows Media Player Fiasco

- Forgot to disclose DVD metadata lookup
- Privacy expert: “MS can track what you watch”
  - Packet sniffer uncovered GUID
  - Scenario wasn’t documented
- Press: “Your secret behavior can be discovered”
  - Porn you watch or pirated media you collect

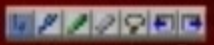
Windows Media Player Fiasco

- Forgot to disclose DVD metadata lookup
- Privacy expert: "MS can track what you watch"
  - Packet sniffer uncovered GUID
  - Scenario wasn't documented
- Press: "Your secret behavior can be discovered"
  - Porn you watch or pirated media you collect
- MS: "We don't collect PII" – but we did!
  - User's email address accidentally commingled with GUID



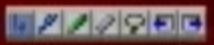
Windows Media Player Fiasco

- Forgot to disclose DVD metadata lookup
- Privacy expert: "MS can track what you watch"
  - Packet sniffer uncovered GUID
  - Scenario wasn't documented
- Press: "Your secret behavior can be discovered"
  - Porn you watch or pirated media you collect
- MS: "We don't collect PII" – but we did!
  - User's email address accidentally commingled with GUID
- Shared metadata cache not easily deleted



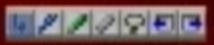
Fire Drill Was Painful

- Reinforced perception we are not trustworthy
  - Catalyst for conspiracy theories
- Left us open to penalties and legal action
- Very disruptive
  - 94 emails first day, multiple people sucked in
- Detailed privacy information incomplete
  - Had to turn statement in 24 hrs
  - Unsure cookie contents and use
- Response wasn't coordinated
  - Too many cooks - "Jumped the gun" on replies

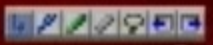


Fire Drill Was Painful

- Reinforced perception we are not trustworthy
  - Catalyst for conspiracy theories
- Left us open to penalties and legal action
- Very disruptive
  - 94 emails first day, multiple people sucked in
- Detailed privacy information incomplete
  - Had to turn statement in 24 hrs
  - Unsure cookie contents and use
- Response wasn't coordinated
  - Too many cooks - "Jumped the gun" on replies

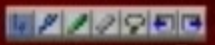


DMD's Holistic Privacy Strategy



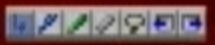
DMD's Holistic Privacy Strategy

- **Optimize "Reactive" Privacy Response**
  - Create Privacy Response Team and process to improve effectiveness



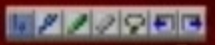
DMD's Holistic Privacy Strategy

- **Optimize "Reactive" Privacy Response**
  - Create Privacy Response Team and process to improve effectiveness
- **"Proactively" address compliance during development**
  - Assign Privacy Leads to analyze and document practices, hold reviews



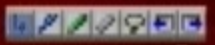
DMD's Holistic Privacy Strategy

- **Optimize "Reactive" Privacy Response**
  - Create Privacy Response Team and process to improve effectiveness
- **"Proactively" address compliance during development**
  - Assign Privacy Leads to analyze and document practices, hold reviews
- **Increase End User trust**
  - Revisit default experience (OOBE), opt-in paradigm, and quality of disclosure



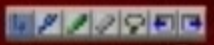
DMD's Holistic Privacy Strategy

- **Optimize "Reactive" Privacy Response**
  - Create Privacy Response Team and process to improve effectiveness
- **"Proactively" address compliance during development**
  - Assign Privacy Leads to analyze and document practices, hold reviews
- **Increase End User trust**
  - Revisit default experience (OOBE), opt-in paradigm, and quality of disclosure
- **Investigate a Windows Privacy Architecture**
  - Make it easier to achieve and maintain compliance



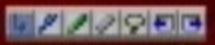
DMD's Holistic Privacy Strategy

- **Optimize "Reactive" Privacy Response**
  - Create Privacy Response Team and process to improve effectiveness
- **"Proactively" address compliance during development**
  - Assign Privacy Leads to analyze and document practices, hold reviews
- **Increase End User trust**
  - Revisit default experience (OOBE), opt-in paradigm, and quality of disclosure
- **Investigate a Windows Privacy Architecture**
  - Make it easier to achieve and maintain compliance



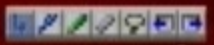
Ways To Increase End User Trust

- Protect privacy by default
  - Media Library not shared
- Present the "value proposition" and opt-in at the time the feature could be used
  - At DVD insert, offer to get metadata.
- Provide adequate controls
  - Turn off internet access by DRM
- Offer detailed disclosure when asked
  - "Phone Home" analysis to concerned customers

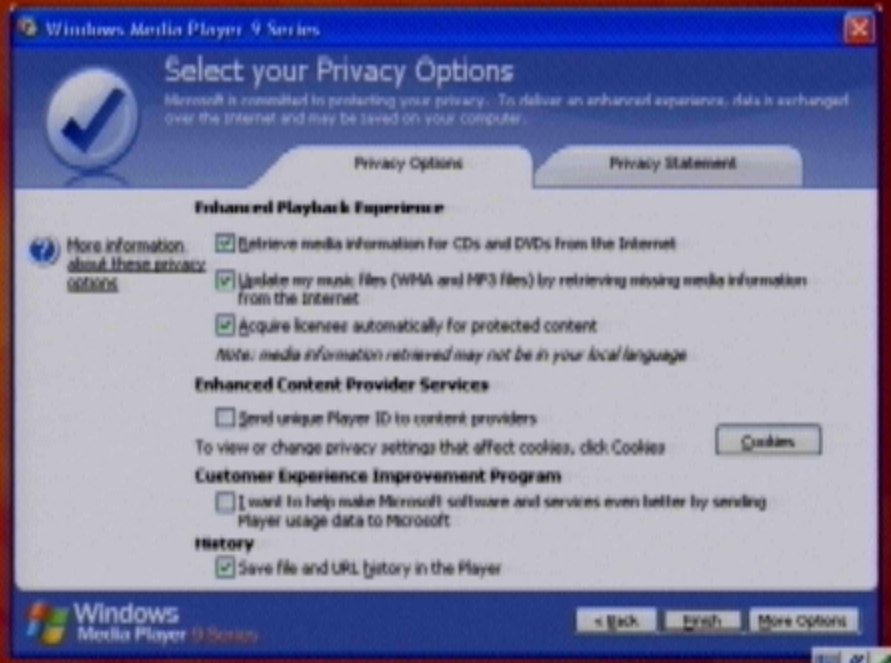


Windows Media Player 9 Series Privacy Enhancements

- Put end users in control right from the start
  - Per user "First Run" Privacy Options dialog
- Changed architecture to enable privacy
  - Per user Media Library can be made private
    - Via built-in XP encryption (EFS) and file permissions (ACLs)
- Added new privacy controls
  - Metadata retrieval switch for CD / DVD and Music Files
  - Do not collect history and clear what's been stored
  - Group policy to disable DRM internet access
- Privacy protected by default
  - Must now opt-in to "uniquely identify my player"

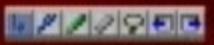


Windows Media Player 9 Series Per User 1st Run Experience

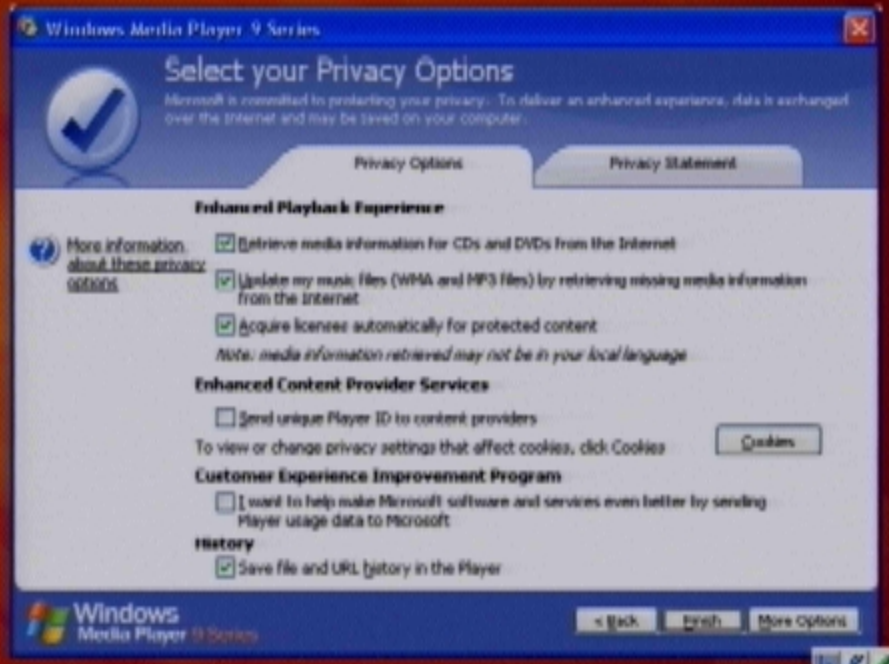


Did It Make a Difference?

- *CNet Article:* **Microsoft breaks new ground** *... Gartenberg, Jupiter analyst: "Few companies offer the same level of privacy opt-in ... Often, privacy policies are hidden in license agreements that run longer than the Magna Carta and are seldom read by users ...* **Microsoft is taking consumer privacy very seriously indeed and marks a big change for the company**."
- *David Chernicoff:* "*...* **the Chicken Littles of the world who were expecting WMP 9 to significantly invade user privacy will be disappointed**."
- *Mike Goslin, influential power user: ... every one of the privacy issues I had been concerned with in the past was an "opt in" option.* **What a huge improvement! ... I can strongly recommend upgrading."**
- *Washington Post:* "*... [The player includes]* **a refreshingly clear explanation of your privacy options and no sneaky attempts to spam you with marketing pop-ups. Other media-software developers -- yes, RealNetworks, that means you -- could learn from this.**

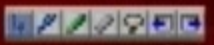


Windows Media Player 9 Series Per User 1st Run Experience

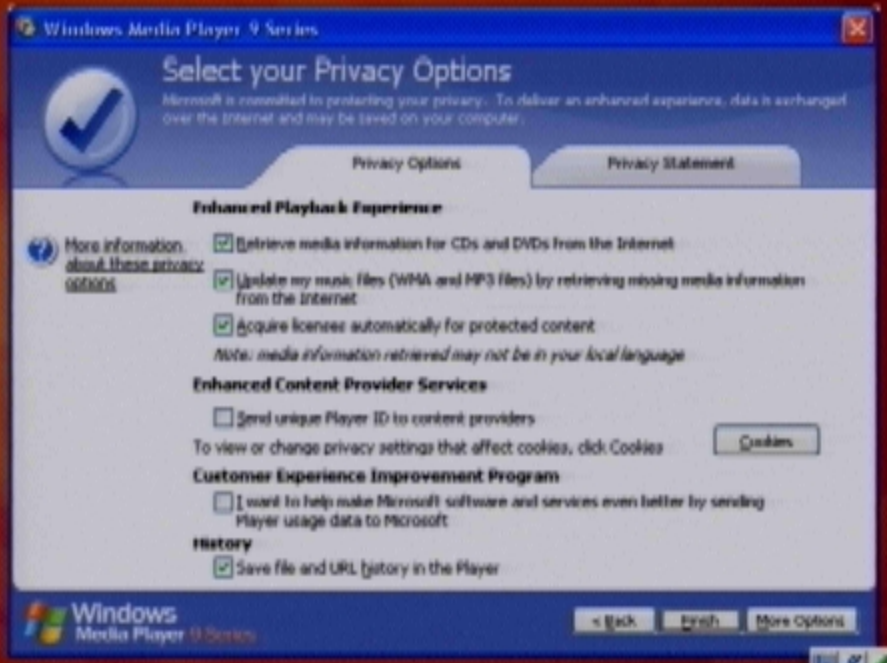


Did It Make a Difference?

- *CNet Article:* **Microsoft breaks new ground** *... Gartenberg, Jupiter analyst: "Few companies offer the same level of privacy opt-in ... Often, privacy policies are hidden in license agreements that run longer than the Magna Carta and are seldom read by users ...* **Microsoft is taking consumer privacy very seriously indeed and marks a big change for the company**."
- *David Chernicoff:* "*...* **the Chicken Littles of the world who were expecting WMP 9 to significantly invade user privacy will be disappointed**."
- *Mike Goslin, influential power user: ... every one of the privacy issues I had been concerned with in the past was an "opt in" option.* **What a huge improvement! ... I can strongly recommend upgrading."**
- *Washington Post:* "*... [The player includes]* **a refreshingly clear explanation of your privacy options and no sneaky attempts to spam you with marketing pop-ups. Other media-software developers -- yes, RealNetworks, that means you -- could learn from this.**

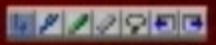


Windows Media Player 9 Series Per User 1st Run Experience



Windows Privacy Initiative

- Proactive compliance with MS policies
  - Drive lifestyle changes across Windows development
  - Establish Windows Privacy Standard
  - Deliver comprehensive Windows privacy statement
- Technology investments
  - Consistent Windows privacy experience
  - Privacy tools for development teams
- Responsiveness
  - Establish Windows Privacy Response framework with Microsoft Privacy Response Center
- Industry leadership
  - Drive privacy technology standards and best practices
  - Influence public policy



Privacy Cabinet

Drives overall initiative:

- Owns Windows Privacy Standard
- Consults / Trains Privacy Leads
- Reviews / Approves privacy exceptions
- Delivers comprehensive Windows Privacy Statement
- Coordinates top-down privacy response

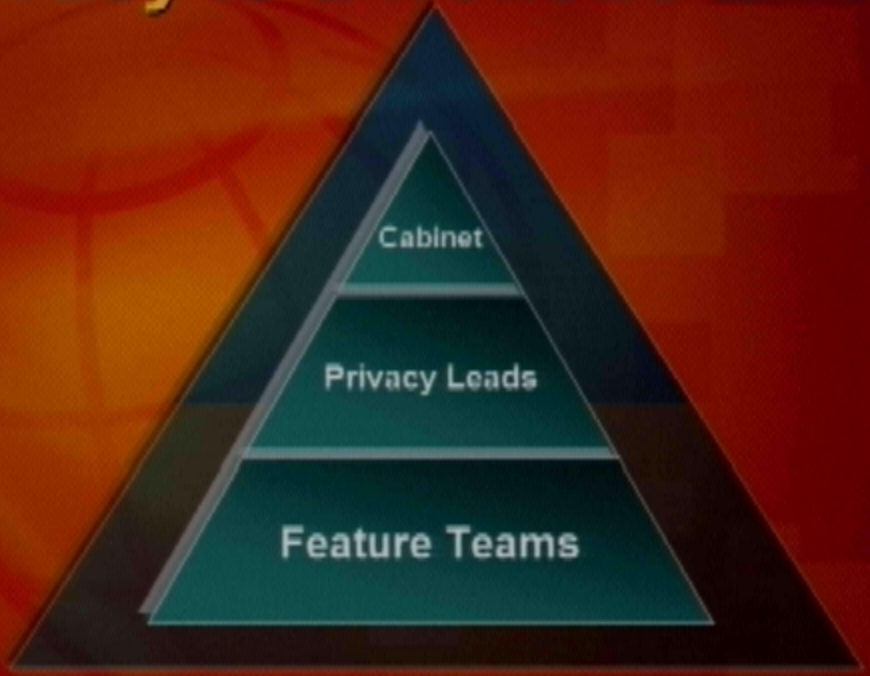
Feature Teams

Internalize and execute:

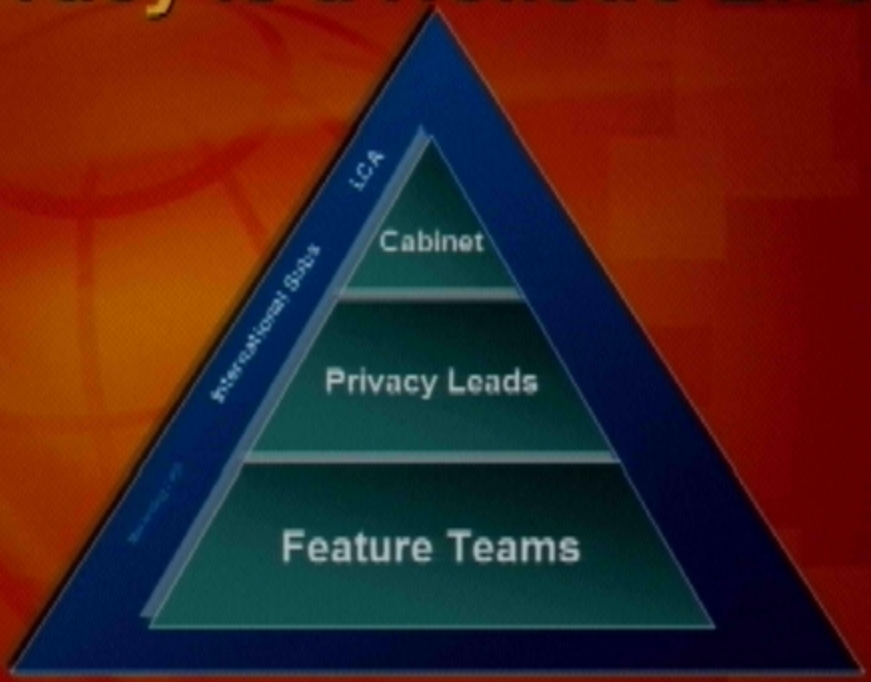
- Complete Privacy Analysis for all features
- Implement appropriate Privacy Controls and Disclosures
- Complete Privacy Testing

Privacy is a Holistic Effort

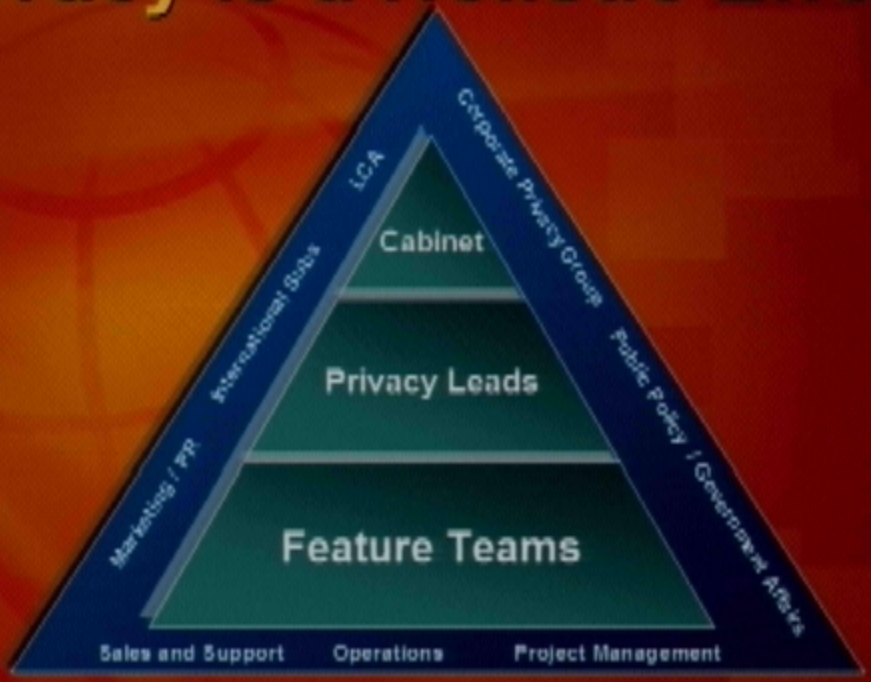
Privacy is a Holistic Effort



Privacy is a Holistic Effort



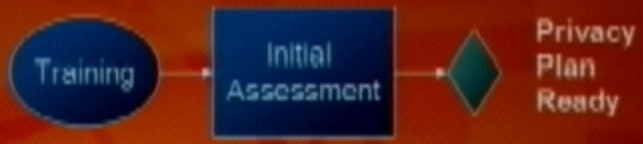
Privacy is a Holistic Effort



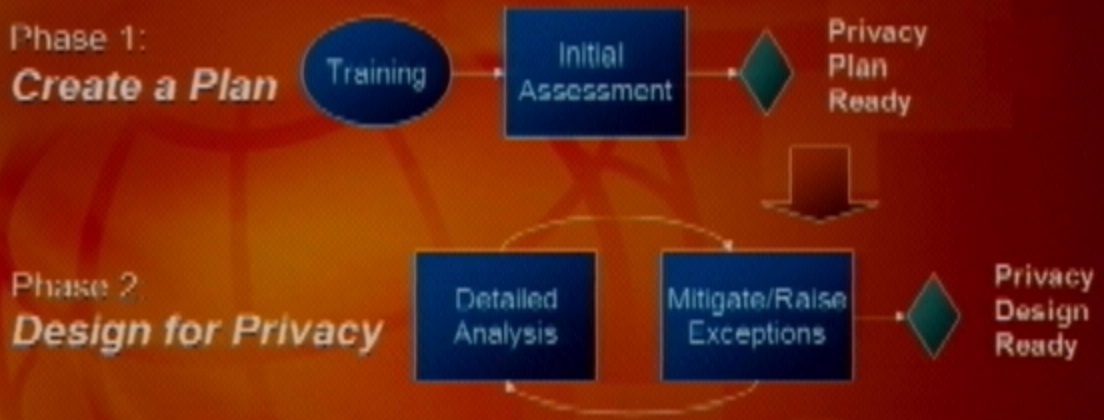
Privacy Process

Privacy Process

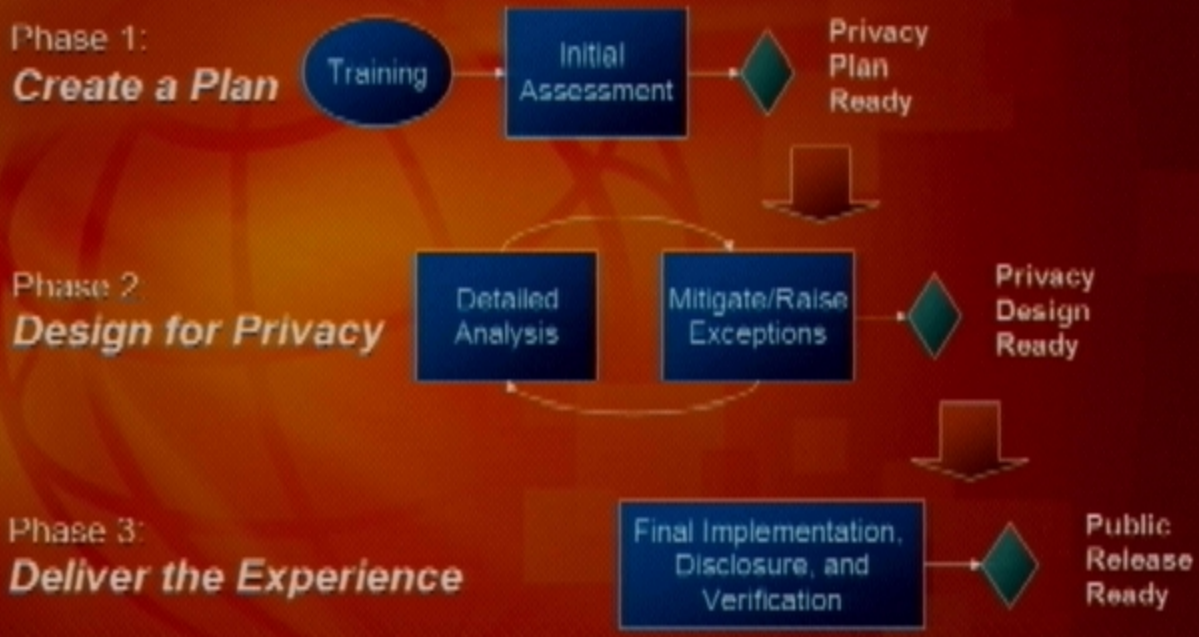
Phase 1:
Create a Plan



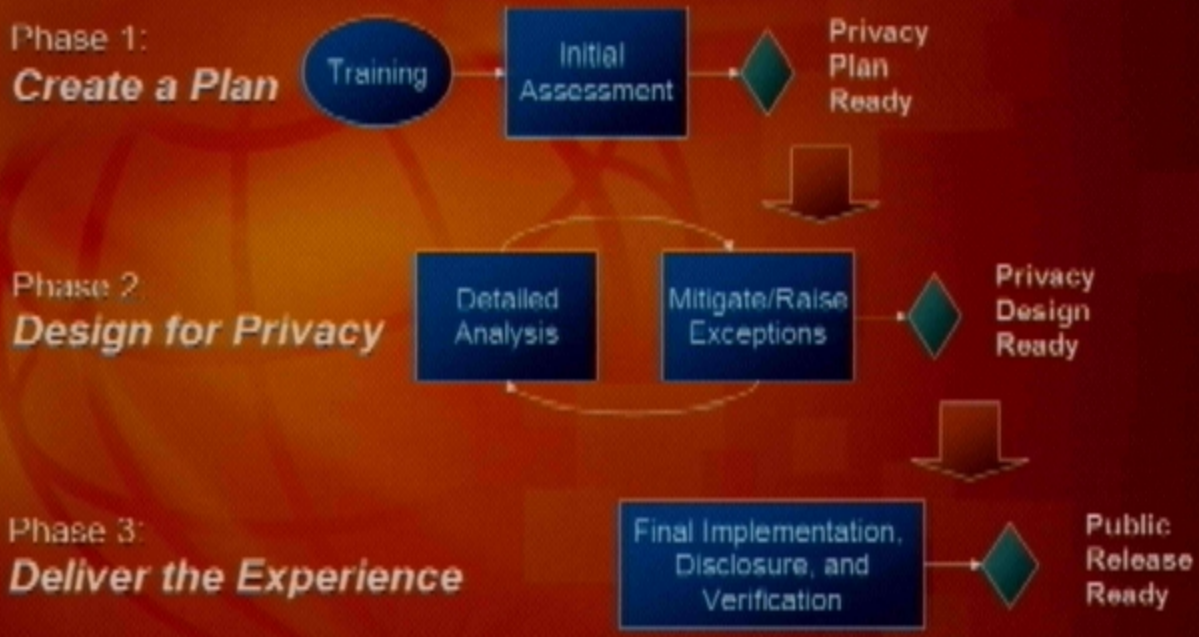
Privacy Process



Privacy Process

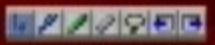


Privacy Process



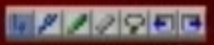
Windows Privacy Standard

- Provides single reference for development
  - Distills best practices and requirements from many sources
  - Complies with Microsoft Corporate Privacy Policy (per CPG)
- Makes development process more efficient
  - Feature Teams can correct their own designs
  - Reviews can focus on exceptions



WPS Data Classes

- Sensitive Data
  - Could facilitate identity theft (SS#, passwords, DOB, …)
  - Could be used to discriminate (beliefs, preferences, …)
- Personal Data
  - Could be traced to a user (email / IP address, serial # …)
  - Tracks a user's behavior (MRU file lists, …)
- Non-Personal Data
  - Anonymous data (aggregated statistics, …)

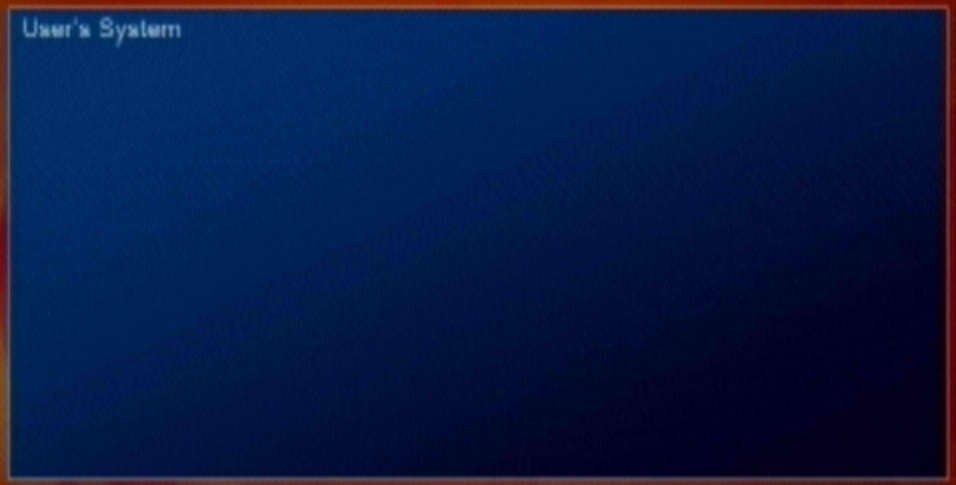


WPS Data Classes

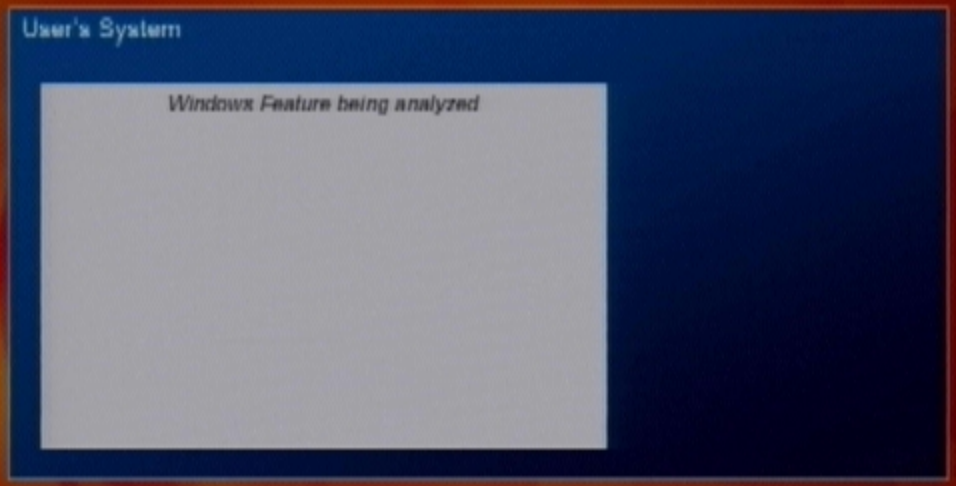
- Sensitive Data
  - Could facilitate identity theft (SS#, passwords, DOB, …)
  - Could be used to discriminate (beliefs, preferences, …)
- Personal Data
  - Could be traced to a user (email / IP address, serial # …)
  - Tracks a user's behavior (MRU file lists, …)
- Non-Personal Data
  - Anonymous data (aggregated statistics, …)

Beware of correlation and commingling!
GUIDs make the data pseudonymous and therefore Personal Data.

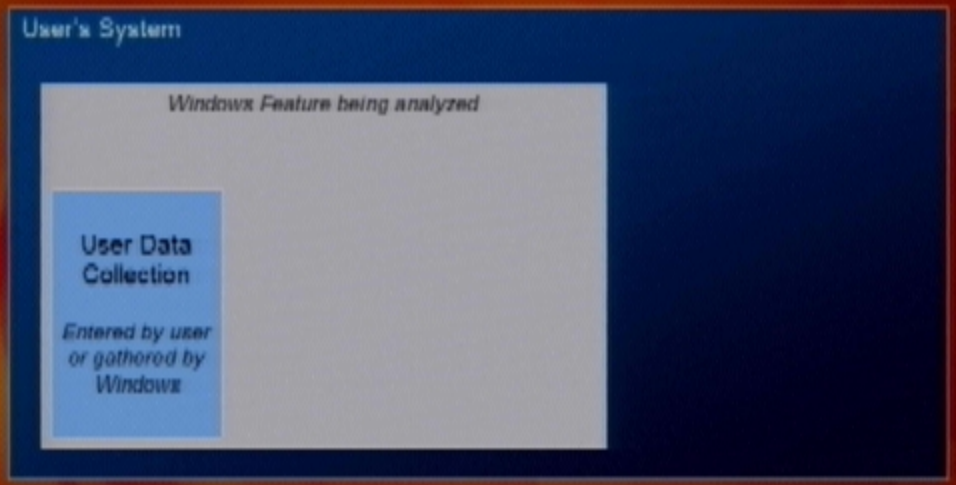
WPS Privacy Model



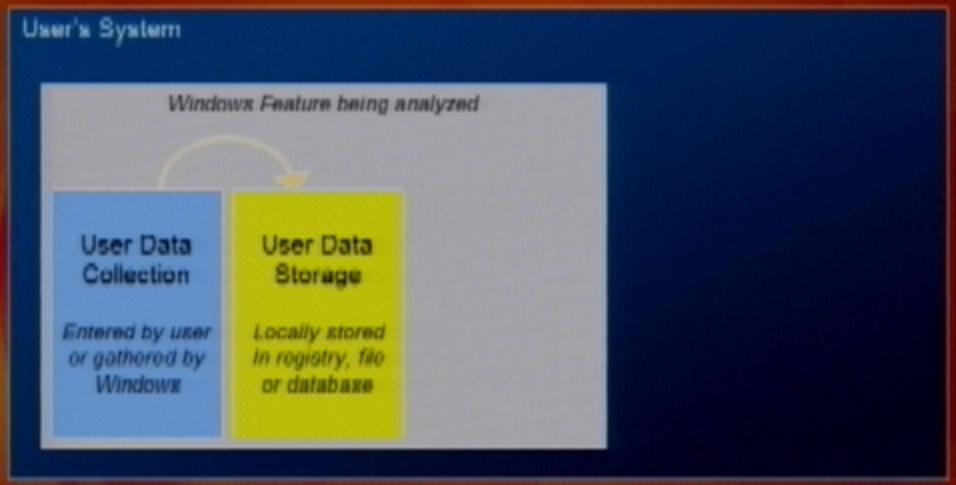
WPS Privacy Model



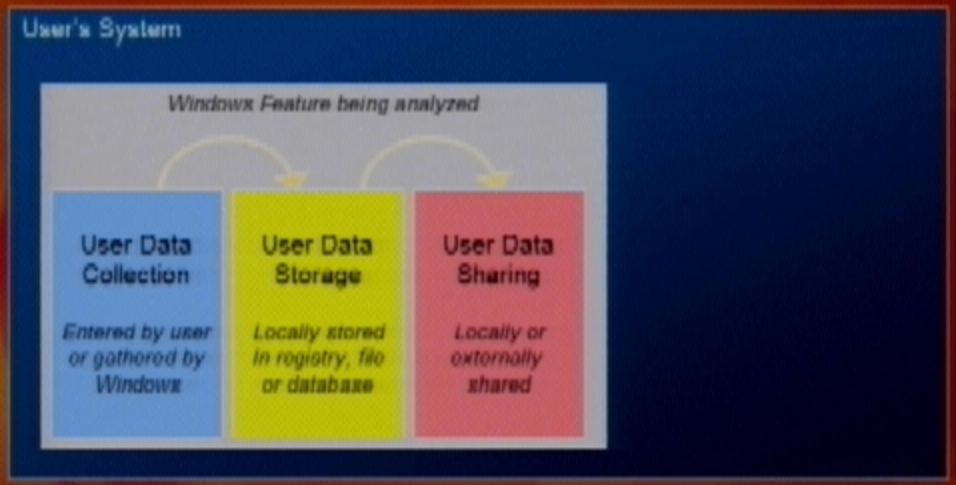
WPS Privacy Model



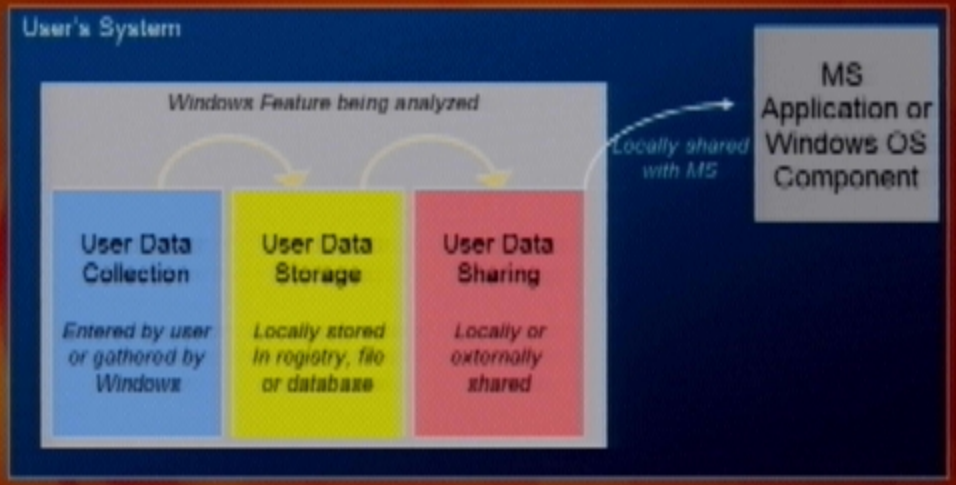
WPS Privacy Model



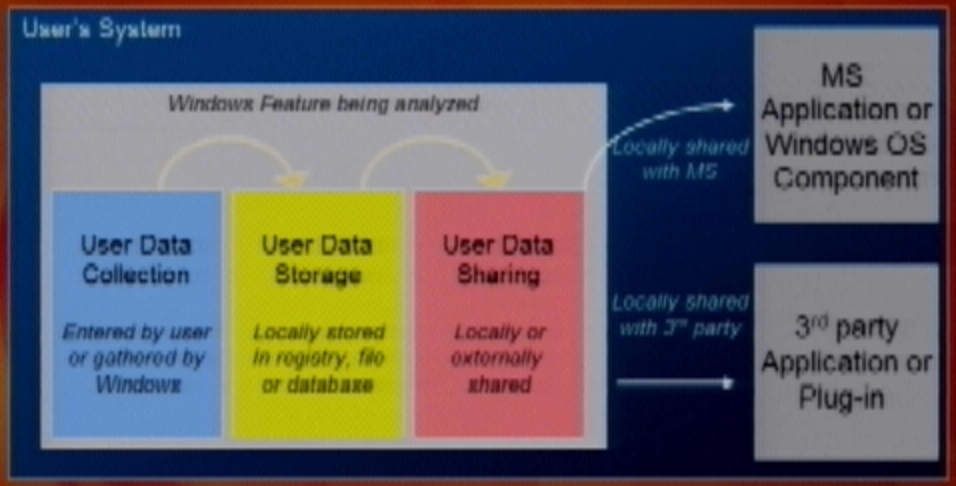
WPS Privacy Model



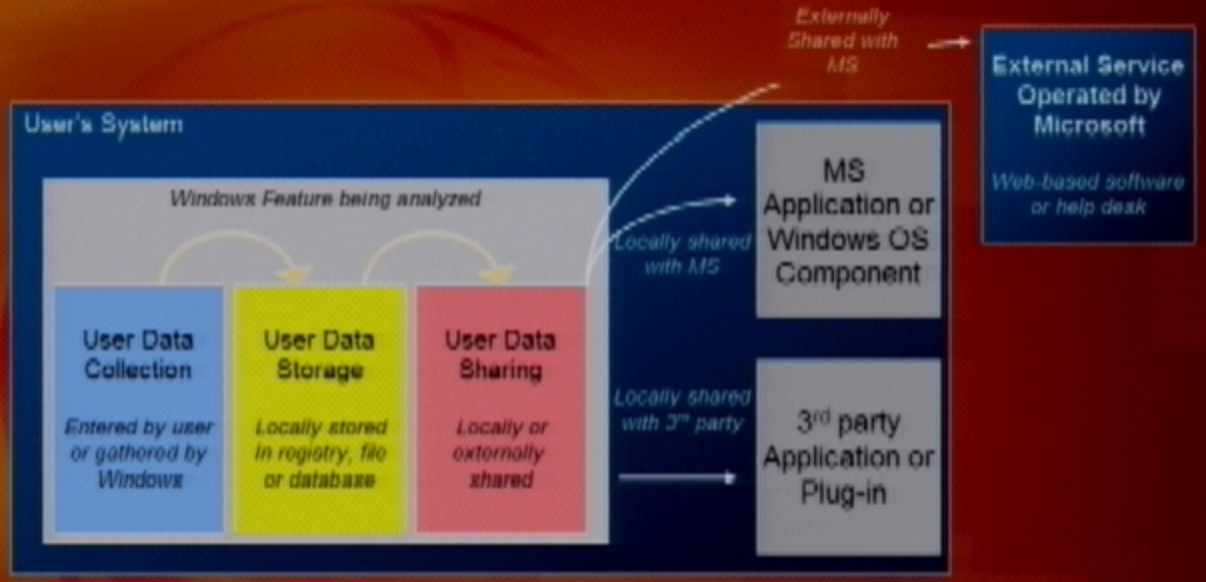
WPS Privacy Model



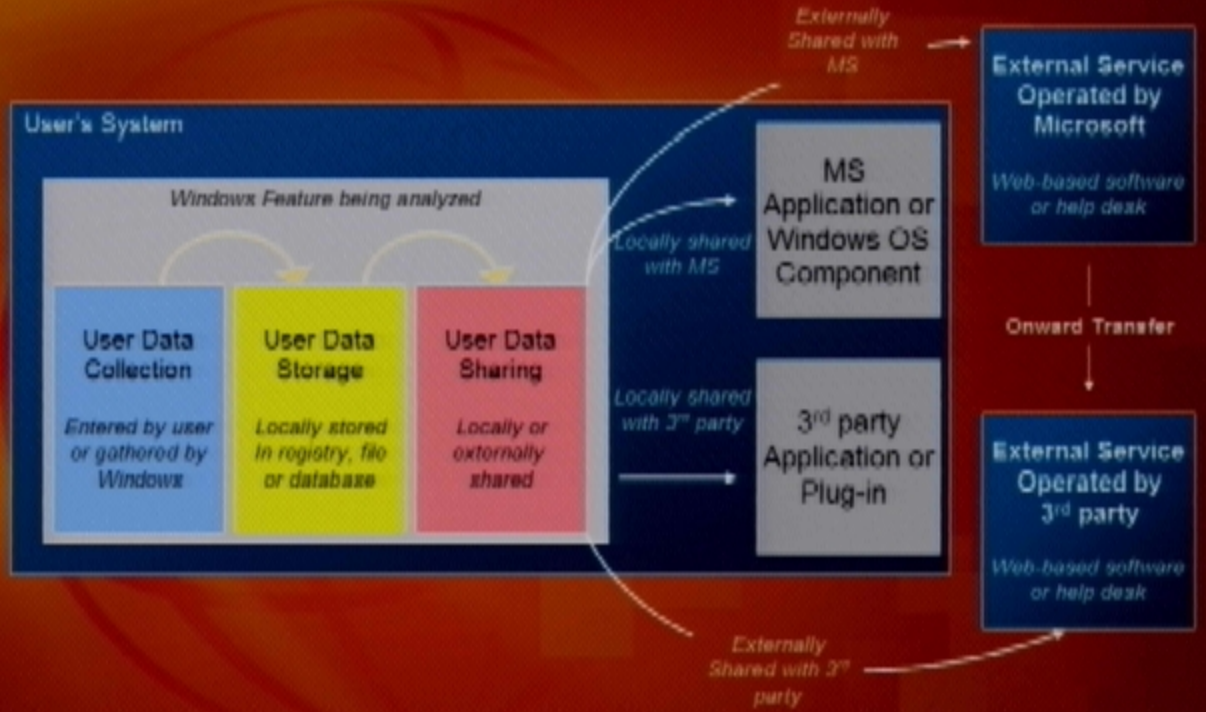
WPS Privacy Model



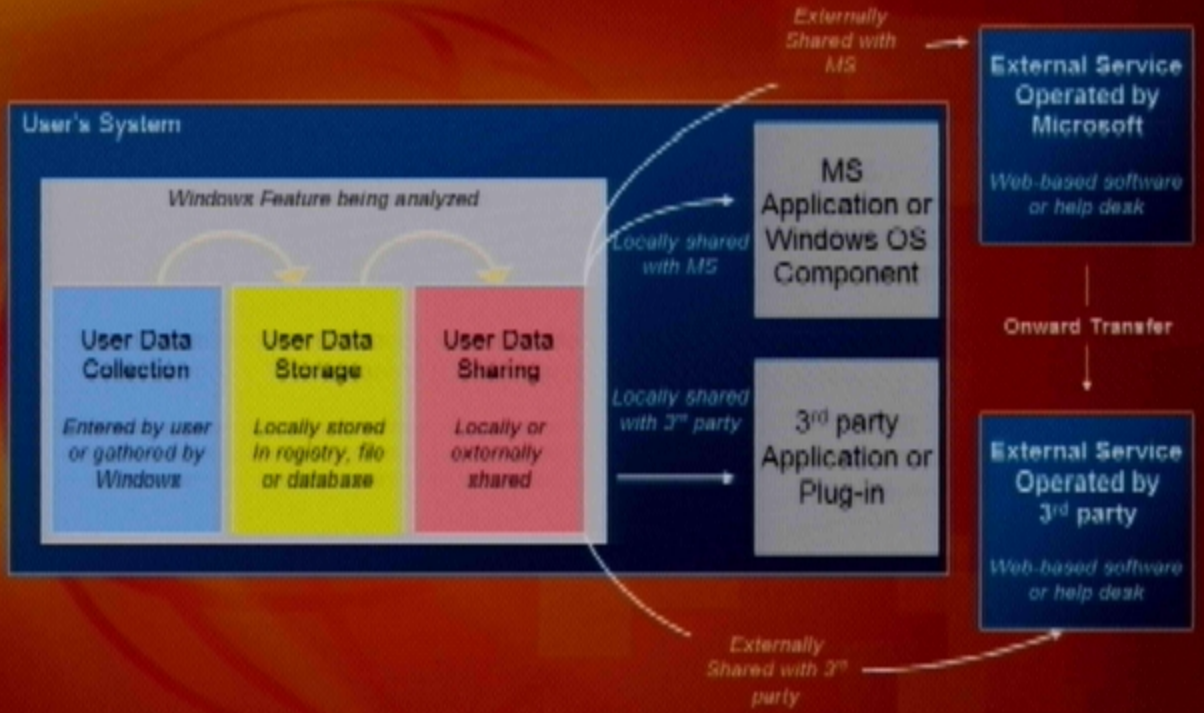
WPS Privacy Model



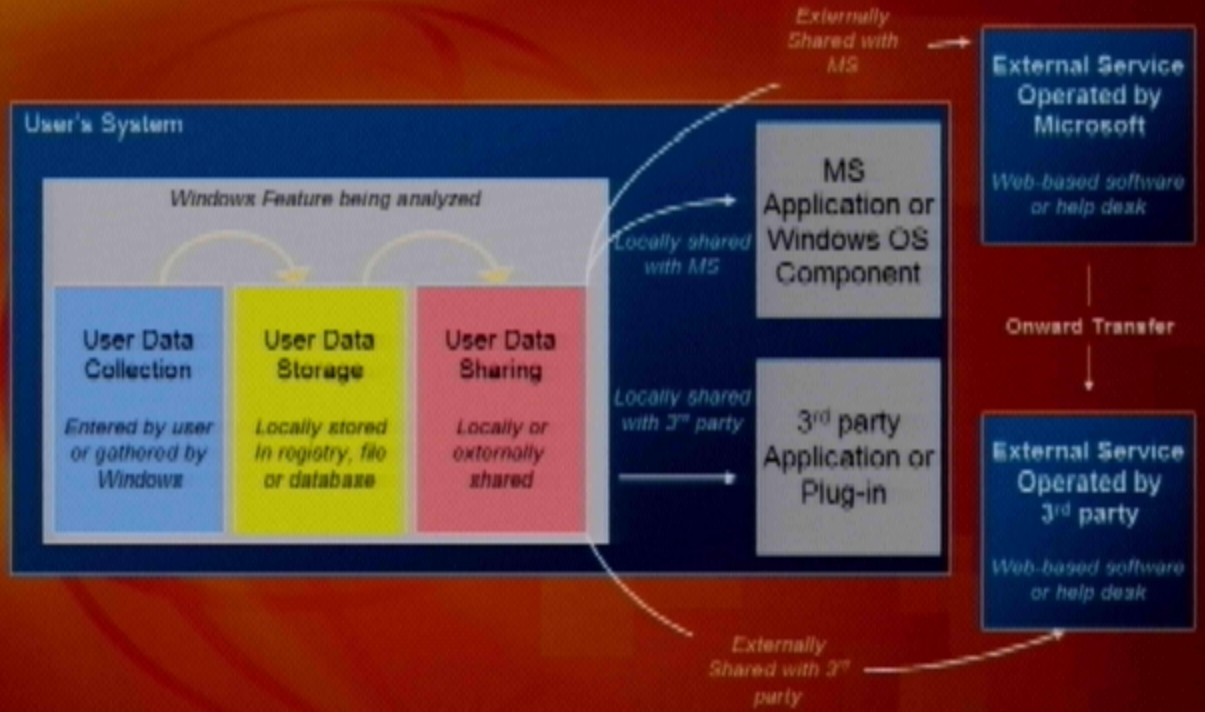
WPS Privacy Model



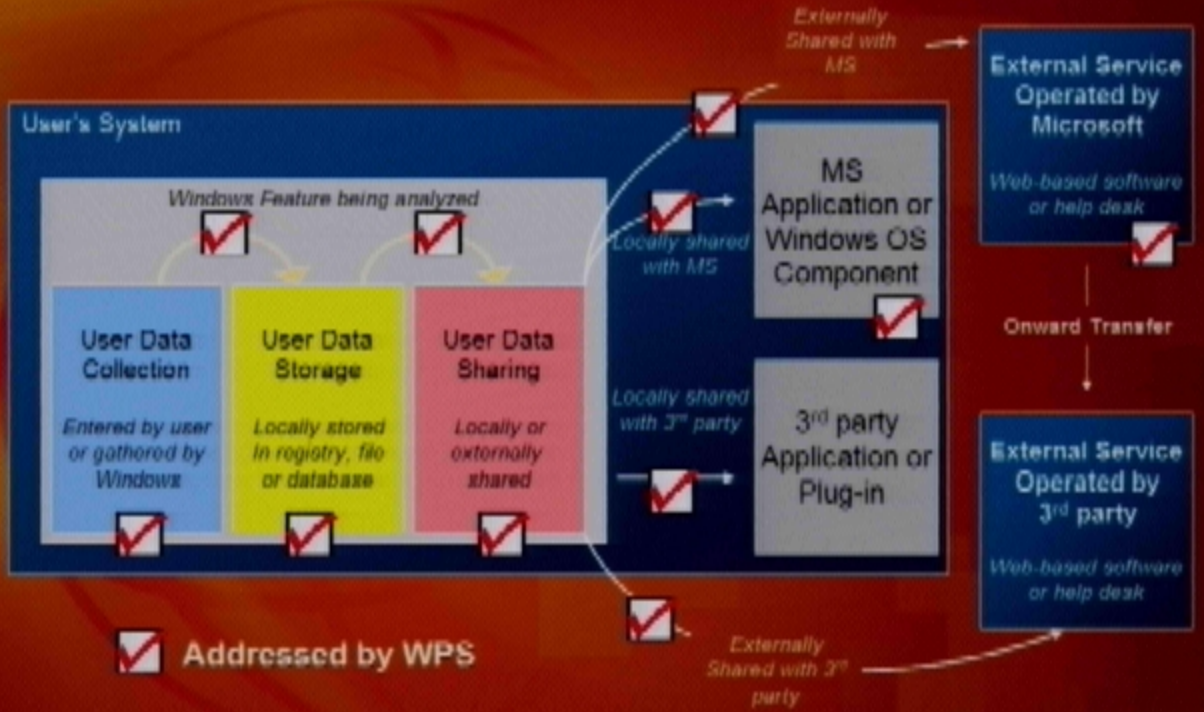
WPS Privacy Model



WPS Privacy Model

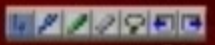


WPS Privacy Model



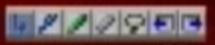
Handling Sensitive Data

- If you collect, store, or share sensitive data, your feature
  - Must provide Prominent Notice and obtain consent before collecting, storing, or sharing, the data
  - Must be disabled by default
    - User must "opt-in"
  - Must protect the data
    - Via ACL and/or encryption



Critical Rules

- Must have clear business justification and customer value proposition
- Must use least sensitive and smallest amount of user data to support feature or business objective
- Must have a privacy control to enable/disable feature
- Must allow domain admin to set and lock defaults
- Must provide appropriate level of disclosure

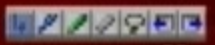


Handling Sensitive Data

- If you collect, store, or share sensitive data, your feature
  - Must provide Prominent Notice and obtain consent before collecting, storing, or sharing, the data
  - Must be disabled by default
    - User must “opt-in”
  - Must protect the data
    - Via ACL and/or encryption

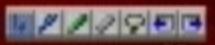
Critical Rules

- Must have clear business justification and customer value proposition
- Must use least sensitive and smallest amount of user data to support feature or business objective
- Must have a privacy control to enable/disable feature
- Must allow domain admin to set and lock defaults
- Must provide appropriate level of disclosure



Critical Rules

- Must have clear business justification and customer value proposition
- Must use least sensitive and smallest amount of user data to support feature or business objective
- Must have a privacy control to enable/disable feature
- Must allow domain admin to set and lock defaults
- Must provide appropriate level of disclosure



WPS Feedback

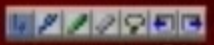
- Are we on the right track?

Longhorn Privacy Investments

- Lifestyle Change
  - Awareness, training, infrastructure, tools
- Detailed Privacy Analysis
  - Make sure practices comply with WPS
- Comprehensive Privacy Statement
- Privacy UX Guidelines
  - OOBE, 1st run, notices, help, …
- "Trust Center"
  - Offers education, status, and control
  - Covers security, privacy, and reliability
- IE P3P Improvements
  - Easier discovery, better summary

Longhorn Privacy Investments

- Lifestyle Change
  - Awareness, training, infrastructure, tools
- Detailed Privacy Analysis
  - Make sure practices comply with WPS
- Comprehensive Privacy Statement
- Privacy UX Guidelines
  - OOBE, 1st run, notices, help, …
- "Trust Center"
  - Offers education, status, and control
  - Covers security, privacy, and reliability
- IE P3P Improvements
  - Easier discovery, better summary



P3P Investments

- Discussion

WPS Feedback

- Are we on the right track?